Content

1 Security Overview .............................................................. 4
   1.1 Business Objects Enterprise Platform Overview ........................ 5
   1.2 LDAP / Active Directory Connectivity ................................... 5

2 User Administration and Authentication in Financial Consolidation .......... 6
   2.1 Using security in SAP Financial Consolidation ......................... 6
   2.2 Managing users using BusinessObjects Enterprise XI authentication . ........ 6
   2.3 Importing and exporting users in the BusinessObjects Enterprise XI platform and the SAP
       BusinessObjects User Management System .............................. 9
       Exporting users with CMSExport ........................................... 9
       Importing users with ImportFromCMS ...................................... 13
   2.4 Connecting to SAP Financial Consolidation using Single Sign On ............. 17
   2.5 Managing the "Enable Excel Pivot Table" Right ............................. 18

3 User Administration and Authentication in Cube Designer .................... 19
   3.1 User Security Implementation Procedure .................................. 19
   3.2 User Implementation Scenarios .............................................. 20
   3.3 Configuring Cube Designer Security into the BOE Platform ................. 21
       Creating User Groups in the Central Management Console .............. 21
       Creating Users .............................................................. 22
       Configuring the EPM Connection Manager Application ................. 23
       Configuring the EPM Connections .......................................... 25
       Configuring Web Intelligence Connections .................................. 26
       Configuring Access Rights on BI Launch Pad Folders .................... 28
       User Rights Table ............................................................ 29
   3.4 Connecting to SSAS Cubes with Third Party Tools .......................... 30
   3.5 Connecting to Cube Designer using Single Sign On .......................... 30

4 Configuring SAP Financial Consolidation Web with firewalls ................. 31
   4.1 Configuring DCOM for firewalls ............................................. 32
       Specifying the recommended configuration .................................. 33
       Specifying a range of ports in DCOM ....................................... 34
       Diagram of the network traffic between the different components ........ 36
       Example of a firewall in use ................................................ 36

5 Restrictions on Uploading Attachments ........................................... 38

6 DCOM configuration .............................................................. 40
   6.1 Checking the default DCOM configuration defined by the SAP Financial Consolidation setup . 41
6.2 Specific DCOM configuration with different domains. ................................................. 43
6.3 Configuring Internet Explorer. .................................................................................... 45

7 Encrypting the settings of the web.config file. .............................................................. 47

8 Installing X.509 certificates. ......................................................................................... 49
  8.1 Installing the X.509 certificate for Cube Deployer. .................................................. 49
  8.2 Installing the X.509 certificate for BFC Monitoring. ............................................... 50

9 EPM Add-in for Microsoft Office Security Settings. ..................................................... 52
  9.1 User Rights. ............................................................................................................. 52
  9.2 Connections. ........................................................................................................... 52
1 Security Overview

EPM applications manages rights within each application, but authentication management is centralized in the BusinessObjects Enterprise XI (BOE) platform.

When you deploy the Financial Consolidation platform, authentication is therefore managed within the BusinessObjects Enterprise (BOE) platform.

**Note**

The internal authentication mode of the Financial Consolidation application is deprecated and therefore, it is strongly recommended to use the BOE authentication. If you want to use Financial Consolidation and Cube Designer components, the internal authentication mode will not function.

You must install one of the following component:

- **BusinessObjects Enterprise XI 4 (BOE XI 4)**
  
  For more information on how to install it, see the SAP web site: http://help.sap.com.

- **Or SAP BusinessObjects Information Platform Services 4.0**
  
  For more information on how to install it, see the SAP BusinessObjects Information Platform Services Installation Guide and the SAP web site: http://help.sap.com.

The SAP BusinessObjects Information Platform Services implements the BusinessObjects Enterprise XI user management sub system. It allows Enterprise Performance Management Solutions to use the BOE authentication without having to install a full BusinessObjects Enterprise XI platform.

The BOE platform is the core component of EPM applications. You can use this component as follows, depending on your environment configuration:

- **The Central Management Console (CMC)** allows you to configure all BOE applications, and also allows end-users to manage their passwords.

- **The SAP Business Objects Cube Designer application in the BOE platform** (also called SAP BusinessObjects EPM Solutions Connection Manager) allows you to manage the Cube Designer application (objects like cubes connections names)

- **The BI Launch Pad application** allows you to publish reports in a web portal.

**Note**

The BI Launch Pad application is not available with SAP BusinessObjects Information Platform Services 4.0.

The use of these different applications depends on the acquired licenses for the EPM Suite; different packages or license keys can be necessary depending on the technical architecture of your environment.
1.1 Business Objects Enterprise Platform Overview

When using the Financial Consolidation application, the following BOE components are also used:

- **EPM Connection Manager Application**: this component manages connectivity, security and authentication between the platform components at a global level.
- **EPM Connections**: this component manages connectivity, security and authentication between the platform components at the level of each "couple" Financial Consolidation database / SSAS database or Financial Consolidation database / NetWeaverBW database, or at the level of EPM Cube Designer used with Profitability and Cost Management and Planning and Consolidation datasources.
- **BI Launch Pad**: this component manages access to the web portal used to store EPM Add-in for Microsoft Office workbooks.
- **Public folders**: this component manages access rights to folders storing reports that you access via BI Launch Pad.
- **Universes**: this component enables access to universes that are automatically created when deploying solutions.
- **Universes Connections**: this component enables access to universes connections that are automatically created when deploying solutions.

**Note**

By default, you cannot see in the CMC the components specifically used by Financial Consolidation Cube Designer. You must install a plug-in (the EPM Connection Manager) to access those components. Once the EPM Connection Manager is installed, the EPM Connections menus will appear in the CMC.

1.2 LDAP / Active Directory Connectivity

When you connect the BOE platform to LDAP or Active Directory, you are also connecting several domains. However, there are some limitations:

- All applications must connect to the BOE platform.
- The BOE platform must connect to the Win/AD directory using Kerberos protocol to manage aliases.
- A "main" domain must be defined. The main domain users will then use their Windows login and other users will have to use a login like "DOMAIN\User".
- It is strongly recommended to configure an SSL protocol, so that Active Directory or LDAP passwords cannot be seen. We recommend that you setup an SSL Protocol on HTTP connections so that Active Directory or LDAP passwords do not appear when a user is logging on to the network.
2 User Administration and Authentication in Financial Consolidation

2.1 Using security in SAP Financial Consolidation

SAP Financial Consolidation enables you to manage users and user security within the BusinessObjects Enterprise XI 4 platform. The security is managed by two settings in the Administration console:

- The `InternalAuthenticationConfigString` key:
  - This key enables you to manage integrated security: users and passwords are managed directly by and in SAP Financial Consolidation.

  **Caution**
  
  You should use this parameter only in one case: when initializing a new empty database, that only contains the ADMIN user but no BusinessObjects Enterprise XI 4 users.

  When security is internally managed by Financial Consolidation, passwords are stored into the database and are encrypted with an RC2 algorithm from the Microsoft API.

- The `ExternalAuthenticationConfigString` key:
  - This key manages the BOE (BusinessObjects Enterprise) Authentication: the users are managed by the BOE XI 4 platform.

  **Caution**
  
  SAP recommends you to use the External authentication mode as the Internal authentication is now deprecated.

2.2 Managing users using BusinessObjects Enterprise XI authentication

**Context**

You must configure BusinessObjects Enterprise XI user authentication in the `External authentication` dialog box when creating a new data source or directly in the `External authentication config string` setting in the `Configuration` page of the administration console.

If authentication is managed by the Business Objects Enterprise XI platform, you must choose the between the two following options:
- Standard external authentication through the Business Objects Enterprise XI platform: you must select the BusinessObjects Enterprise XI authentication option and enter the name of the Central Management Server (CMS) of your BusinessObjects Enterprise XI platform in the CMS server name field.

- External authentication through the BusinessObjects Enterprise XI web service: you must select the BusinessObjects Enterprise XI authentication (Web Service) option and enter the complete web service name in the CMS server name field, as follows: http://CMS-SERVER-NAME:8080/dswsobje/services/session.

**Caution**
This option is mandatory for all other authentication types included those using the BusinessObjects Enterprise XI platform.

If you want to use Single Sign On between EPM applications installed with the same BusinessObjects Enterprise platform, select Activate SSO for Web EPM Suite. When you select this option, a session will be kept open on the CMS during the entire Financial Consolidation session for each Financial Consolidation user. Therefore, you must make sure that your Business Objects Enterprise XI license is for a sufficient number of users.

**Caution**
The following authentication modes are no longer supported by SAP BusinessObjects Financial Consolidation. The only reason they are available is to ensure compatibility with previous versions. You must always use the Business Objects Enterprise authentication, unless you are migrating from a previous SAP BusinessObjects Financial Consolidation version, and your authentication mode must remain the same.

- Active Directory / LDAP authentication
- LDAP authentication
- Script authentication
- Plug-in authentication

**Caution**
If you want to use the LDAP or Active Directory authentication, you must do it into the Business Objects Enterprise XI Central Management Console. Additional authentication modes like SAP NetWeaver are also supported through the BOE XI platform.

**Note**
If your BOE platform uses a CMS cluster, then you need to indicate, in the CMS server name field, all the cluster members, one by one, separated by a coma.

**Procedure**

1. Enter the fields in this dialog box as shown in the example below:
2. **Configure external authentication**: select the Business Objects XI authentication.

3. **CMS server name**: enter the name of the Central Management Server (CMS).

   Once you have defined BusinessObjects Enterprise XI as the authentication provider in the Administration console, you should create SAP Financial Consolidation users corresponding to the BusinessObjects Enterprise XI users.

   You create users in SAP Financial Consolidation as follows:

   4. In the **Users** view, create a new user and select the **Authentication** tab.

   5. Select **Use external authentication** and enter the domain and the BOE user name (DOMAIN\BOE_username) in the **Login** field.

   **Note**

   If you want to use Single Sign On with the EPM Add-in for Microsoft Office or other EPM applications, you must create users in SAP Financial Consolidation as mentioned above, and add the following information in the **Authentication** tab: in the **Alias** area, enter the same alias as the one provided in the properties of the BusinessObjects Enterprise XI user, as indicated below.
Once you have saved this user in SAP Financial Consolidation, he/she will only be able to connect using the BusinessObjects Enterprise XI login and password or to connect directly to the application if Single Sign On has been configured.

### 2.3 Importing and exporting users in the BusinessObjects Enterprise XI platform and the SAP BusinessObjects User Management System

With the CMS tool, you can export SAP Financial Consolidation users to the Central Management Server (CMS) of the BOE XI platform or the SAP BusinessObjects User Management System, and you can import CMS users to SAP Financial Consolidation.

#### 2.3.1 Exporting users with CMSExport

The CMSExport Tool enables you to export the users created in SAP Financial Consolidation to the CMS (Central Management Server) of the BOE platform (Business Objects Enterprise XI) or the SAP BusinessObjects Information Platform Services.
Note

This version only takes into account Financial Consolidation in integrated security mode, with the login and password managed by SAP Financial Consolidation. Users with LDAP, Active Directory or Windows HTML authentication will be considered in a future version.

This tool is composed of:

- An XML configuration file: CMSExportConfiguration.xml
- An .exe file: CMSExport.exe

Once this tool is executed:

- All users of the selected member profiles are taken into account and migrated into the CMS.
- For each migrated user, a corresponding user with the same login and a new randomly generated password (except if one already exists) is created in the CMS.
- The existing Financial Consolidation users are associated with the new CMS logins created in the platform.
- Each new CMS user will also be associated with a specific group, depending on the Financial Consolidation functional profiles defined in the configuration file of the tool.

Caution

It is the responsibility of the BOE administrator to set the relevant functional rights. The tool will NOT apply any functional rights to the migrated users and groups. The rights must be set manually.

2.3.1.1 Structure of the XML file

The file is located at the root of the SAP Financial Consolidation installation folder. By default, C:\Program Files (x86)\SAP\Financial Consolidation.

```xml
<?xml version="1.0" encoding="utf-8"?>
<CMSExportConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    <FinanceFonctionalProfiles>
        <Profile>MyFP1</Profile>
        <Profile>MyFP2</Profile>
        <Profile>MyFP3</Profile>
    </FinanceFonctionalProfiles>
    <FinanceDataSource BrokerName="BROKER_MACHINE" DataSourceName="DATASOURCE_NAME" />
    <PasswordLength>8</PasswordLength>
    <ForcePasswordRenewal>false</ForcePasswordRenewal>
    <CMSGroupName>FinancialConsolidation</CMSGroupName>
    <LogFile>exportusers2CMS.log</LogFile>
    <OutputFile>CreatedUsers.csv</OutputFile>
    <UserConnectionType>Named</UserConnectionType>
</CMSExportConfig>
```

This file is composed of the following XML tags:
FinanceFonctionalProfiles

This parameter corresponds to the Financial Consolidation functional profiles that will be processed by the export tool. By default, if empty, all Financial Consolidation users are migrated.

(not Windows et not admin)

FinanceDataSource

This parameter must be filled in with the Financial Consolidation datasource and datasource manager (CtrBroker) names.

PasswordLength

This parameter must be filled in with the password length you want to generate. By default, this is set to eight characters.

ForcePasswordRenewal

This parameter enables you to force the user to change the password at the first connection after migration. It must be filled in with the False or True option. By default, it is set to False.

CMSSGroupName

This parameter must be filled in with the CMS group name. It corresponds to the User Group created in the CMS where all the migrated users are imported. By default, this group is named FinancialConsolidation.

LogFile

This parameter corresponds to the log file that will be generated after execution of the tool. By default, it is named exportusers2CMS.log.
OutputFile

This parameter corresponds to the .csv file generated after the migration and indicating the CMS login names and randomly generated passwords that have been created. By default, the file is named CreatedUsers.csv.

UserConnectionType

This parameter corresponds to two different user types: Named or Concurrent. It depends on the type of license you are using within the BOE platform. By default, this parameter is set to Named.

2.3.1.2 Migration procedure

2.3.1.2.1 Requirements before executing the migration

⚠️ Caution

Before migrating users, make sure that no users are connected and working in the SAP Financial Consolidation application.

1. In the SAP Financial Consolidation administration console, set the external authentication parameter to BusinessObjects XI authentication.
2. Enter a login in the XML file which is an SAP Financial Consolidation user defined as an administrator in his user profile and configured with the external authentication and with administration rights on the BOE platform.

👉 Tip

It is recommended that you create a user to execute the migration. Do not use the Financial Consolidation ADMIN login.

2.3.1.2.2 Migration steps

Procedure

1. Execute the tool from the server where the Data Source Manager is located (where the CtBroker.exe process runs).
2. Edit the XML file.
3. Complete the XML file with the relevant parameters, depending on the configuration of your SAP Financial Consolidation and Cube Designer applications.
4. Save the file.

5. Open the Command Prompt selecting *Run as administrator*.

6. From the Financial Consolidation installation folder, execute the following command line:

   CMSExport.exe CMSExportConfiguration.xml FC_USER_NAME \[FC_USER_PASSWORD\]

   FC_USER_NAME: this parameter corresponds to the login name that is used to connect to Financial Consolidation and to the CMS.

   FC_USER_PASSWORD: this parameter corresponds to the user login above. If there is no password associated to the login, you can skip this parameter in the command line.

   **Caution**

   This user must have administrator rights on the Financial Consolidation platform AND on the Central Management Server of the BOE platform or Information Platform Services. Do not use the Financial Consolidation ADMIN login.

7. Verify that all users have been properly deployed to the CMS.

8. Set the relevant functional rights in the Central Management Console, depending on the user groups you want to define.

   **Caution**

   A user with multiple functional rights in Financial Consolidation will probably be deployed into several different user groups in the CMS.

### 2.3.2 Importing users with ImportFromCMS

The ImportFromCMS Tool enables you to import users created in the Central Management Server (CMS) of the BOE platform (Business Objects Enterprise XI) or SAP BusinessObjects Information Platform Services to SAP Financial Consolidation.

**Note**

This version only takes into account Financial Consolidation in integrated security mode, with the login and password managed by SAP Financial Consolidation.

This tool is composed of:

- An XML configuration file: ImportFromCMSConfiguration.xml
- An .exe file: ImportFromCMS.exe

Once this tool is executed:

- The CMS group is processed. All CMS user members of the CMS group are taken into account and migrated into SAP Financial Consolidation.
- Each user is attributed a Financial Consolidation user login and password as specified in the XML configuration file.
- For each migrated user, a corresponding Financial Consolidation broker and data source, level, owner group, functional profile and data access group is attributed, a specified in the XML configuration file.
• Each new user has a status of either active or inactive.
• A log file is created, detailing all of the operations.
• A .csv file is created, listing all of the users migrated to Financial Consolidation and the associated CMS login names.

2.3.2.1 Structure of the XML file

The file is located at the root of the SAP Financial Consolidation installation folder. By default, C:\Program Files (x86)\SAP\Financial Consolidation.

```xml
<?xml version="1.0"?>
  <FinanceFonctionalProfiles>
    <Profile>MyFP1</Profile>
    <Profile>MyFP2</Profile>
  </FinanceFonctionalProfiles>
  <CMSGroup>CMSUsersGroup</CMSGroup>
  <FinanceDataAccessGroup>FDAG</FinanceDataAccessGroup>
  <FinanceUserActive>true</FinanceUserActive>
  <FinanceLevel>Standard</FinanceLevel>
  <LogFile>ImportFromCMS.log</LogFile>
  <OutputFile>CreatedUsers.csv</OutputFile>
  <FinanceGroups>
    <Group>FCGroup</Group>
  </FinanceGroups>
</ImportFromCMSConfig>
```

This file is composed of the following XML tags:

**FinanceFonctionalProfiles**

This parameter corresponds to the Financial Consolidation functional profiles that will be processed by the import tool. This parameter is mandatory.

**FinanceDataSource**

BrokerName: Financial Consolidation broker computer name. This parameter is mandatory.

DataSourceName: Financial Consolidation data source name. This parameter is mandatory.
CMSGroup

This parameter corresponds to the CMS group name containing the CMS users to take into account. This parameter is mandatory.

FinanceDataAccessGroup

This parameter corresponds to the name of the Financial Consolidation Data Access group to set for the created user. This parameter is mandatory.

FinanceUserActive

This parameter specifies if the user created will be active or inactive. The default value is "True".

FinanceLevel

This parameter must be filled in with the Financial Consolidation user level for the newly created Financial Consolidation users. The default value is "Standard".

LogFile

This parameter corresponds to the log file that will be generated after execution of the tool. The default value is ImportFromCMS.log.

OutputFile

This parameter corresponds to the .csv file generated after the migration and indicating the Financial Consolidation login names and randomly generated passwords that have been created. The default value is CreatedUsers.csv.

Group

This parameter must be filled in with the Financial Consolidation owner group name. This parameter is mandatory.
2.3.2.2 Migration procedure

2.3.2.2.1 Requirements before executing the migration

The SAP Financial Consolidation data source must have external authentication set to Business Objects, with a valid CMS specified.

The Financial Consolidation user that executes the migration must have SAP Financial Consolidation user administration rights.

Users created in SAP Financial Consolidation using the import tool are created with options defined in the XML configuration file.

2.3.2.2.2 Migration steps

Procedure

1. Execute the tool from the server where the Data Source Manager is located (where the CtBroker.exe process runs).
2. Edit the XML file.
3. Complete the XML file with the relevant parameters, depending on the configuration of your SAP Financial Consolidation and Cube Designer applications.
4. Save the file.
5. Open the Command Prompt selecting Run as Administrator.
6. From the Financial Consolidation installation folder, execute the following command line:
   \ImportFromCMS.exe ImportFromCMSConfiguration.xml FC_USER_NAME [FC_USER_PASSWORD]
   FC_USER_NAME: this parameter corresponds to the login name that is used to connect to Financial Consolidation and to the CMS.
   FC_USER_PASSWORD: this parameter corresponds to the user login above. If there is no password associated to the login, you can skip this parameter in the command line.

   **Caution**

   This user must have administrator rights on the Financial Consolidation platform AND on the Central Management Server of the BOE platform or Information Platform Services. Do not use the Financial Consolidation ADMIN login.

7. Verify that all users have been properly migrated to SAP Financial Consolidation.
2.3.2.3 Importing Active Directory Users from the BOE Platform

If the users you want to import from the BOE platform are configured with Active Directory syntax, you must take into account the following:

Active Directory can be used with two syntaxes:

- Domain\user
- username@domainname

If the BOE platform uses the second syntax, when importing users, the import tool will retrieve this syntax. Since this second syntax is not recognized by the Financial Consolidation application, you must manually change users passwords once the users have been imported into Financial Consolidation database.

2.4 Connecting to SAP Financial Consolidation using Single Sign On

EPM for Finance applications introduce a Single Sign On (SSO) mechanism between web applications. SSO allows a user to sign on to one EPM for Finance web application and then use other EPM web applications without having to enter his credentials.

For example, a user enters his credentials to connect to the SAP BusinessObjects InfoView web portal and he receives a BusinessObjects Enterprise XI session cookie. From SAP BusinessObjects InfoView, he goes to the SAP Financial Consolidation web application with the same browser session, and does not need to re-enter his credentials, he is logged on automatically. His BusinessObjects Enterprise XI session cookie is reused automatically.

A reverse proxy server can be mandatory if you are using single sign-on (SSO).

For SSO to work, follow this procedure:

- Use the SAP BusinessObjects authentication with the same SAP BusinessObjects Enterprise platform for all EPM for Finance applications
- Use the same URL domain name for all EPM for Finance applications web sites:
  - Either all EPM for Finance applications web servers must be installed on the same physical server,
  - or each web application is installed on separated servers and all URLs are published on the same reverse proxy server.

**Note**

To enable the connection on several IE windows instead of on several tabs within the same IE window:

1. Open Internet Explorer.
2. Click **Tools** button (or press `Alt` + `X`).
3. Click **Compatibility View settings**.
4. In **Change Compatibility View Settings** dialog box, copy and paste the SAP Financial Consolidation web URL in **Add this web site** box and click **Add**.
5. Click Close.
6. Close Internet Explorer.

If you are using a multiple web server configuration with a NLB (Network Load Balancing) device, configure the NLB URL in the reverse proxy.

For example, with the Apache application as Reverse Proxy and a Financial Consolidation web application deployed on MyServer, the `httpd.conf` configuration file would have the following lines:

```
ProxyPass /FinancialConsolidation http://MyServer/Finance
ProxyPassReverse /FinancialConsolidation http://MyServer/Finance
```

## 2.5 Managing the "Enable Excel Pivot Table" Right

To use the Excel Links, the user must be granted the "Enable Excel Links" functional right.

In order to create pivot tables inside Excel Links, the user must be granted This right authorizes the Excel Links connect to the database, and therefore to retrieve the database connection information.

⚠️ **Caution**

When this right is enabled, the user has full access to the database, so proceed with caution.
3 User Administration and Authentication in Cube Designer

3.1 User Security Implementation Procedure

Using the second scenario in chapter "Users Implementation Scenarios", the following steps are required:

First step: Configure the EPM Connection Manager security in the BusinessObjects platform.

1. Create the three user groups below:
   ○ CD_Admins
   ○ CD_Designers
   ○ CD_Viewers
2. Create the users you want to assign to these groups.
3. Assign rights and access levels to the EPM Connection Manager, for each group of users. To find out more about those rights, see Configuring the EPM Connection Manager Application [page 23].
4. Assign access levels to the EPM connections that allow users to access the specific Cube Designer objects. To find out more about those rights, see Configuring the EPM Connections [page 25].

Caution

By default, if access rights are not configured, you cannot see any specific folders or objects concerning BOE Cube Designer in the CMC.

Second step: Configure security in each relevant EPM application.

1. Define the corresponding rights in the Financial Consolidation application. Before version 7.5, rights were defined in Financial Consolidation. This is now done in the BOE platform. Cube Designer users must be granted the following rights:
   ○ in the Financial Consolidation application: Analysis > Analytics > Administration.
   ○ In the BOE platform: Design Cubes

Note

If you want to grant a Cube Designer user administration rights, this user must also be granted the Full Control access level.

Note

In the Financial Consolidation application, you manage rights on data via data access groups as in previous versions.
2. Configure the user authentication in the Financial Consolidation administration console.
3. Configure user accounts in Financial Consolidation.

### 3.2 User Implementation Scenarios

As it is complex to manage access rights to different applications for each user, we recommended that you assign access rights to groups, and then to assign users to those groups.

**Note**
It is possible to assign a user to several groups.

Examples of user implementations are:

#### Scenario 1

- **Everyone:**
  Those users can log on to the Business Objects Enterprise platform, but have no rights on applications deployed into the platform. It can be used for users connecting to EPM applications, with Business Objects Enterprise authentication.
- **Designers (CubeDesignerDesign):**
  This user group can create and deploy cubes into Designer.
- **Publishers (CubeDesignerPublish):**
  This user group can connect to BI Launch Pad and to publish Excel spreadsheets in public folders.
- **Analysts (CubeDesignerAnalyze):**
  This user group can connect to BI Launch Pad and use the EPM-Addin for Microsoft Office but not to modify documents that are published into public folders.

#### Scenario 2

- **Admin (CD_Admins):**
  This user group has full rights.
- **Designers (CD_Designers):**
  This user group has the rights to publish, analyze and design cubes in Designer.
- **Viewers (CD_Viewers):**
  This user group can connect to BI Launch Pad and publish Excel workbooks in public folders.
3.3 Configuring Cube Designer Security into the BOE Platform

3.3.1 Creating User Groups in the Central Management Console

Context

You can create groups and then assign users to those groups, so that you manage security for one group instead of many users. If you want to use the previous scenario, create the following groups:

- CD_Admins
- CD_Designers
- CD_Viewers

Procedure

1. Log on to the Central Management Console and click Users and Groups.
2. Click Manage > New > New Group.
3. Enter a group name, in our example “CD_Designers” and a description.
4. Click OK.
5. Create groups named “CD_Viewers” and “CD_Admins” following the same steps.
3.3.2 Creating Users

Context

Once the groups are created, you add the users. In this section, "CD_User_1" will be created and assigned to the CD_Designers group.

Procedure

1. Log on to the Central Management Console and in the Organize section, click Users and Groups.
2. Select Manage > New > New User and create a new user. For our example, this user is named "CD_User_1".
3. Select the following User role: BI Analyst User.
4. Click Save and close.
5. In the User List, right-click this new user and select Join Group.
   The Join Group: CD_User_1 window opens.
6. Click Join Group.
7. In the Group List, select CD_Designers and add it to the Destination Group(s) by clicking >.
8. Click OK.
9. Repeat the same steps to create other users. For this example, you need to add all the users of your environment to the three groups created before:

- CD_Admins
- CD_Designers
- CD_Viewers

Note
You can select several users once a time by using the Ctrl or Shift / Caps.

Note
When migrating, the CMSExport Tool enables you to automatically export the users created in Financial Consolidation to the CMS (Central Management Server) of the BOE platform.

### 3.3.3 Configuring the EPM Connection Manager Application

#### Context

This chapter explains how to assign rights and access levels to the EPM Connection Manager application in the BOE.

When using scenario 2, provided in this documentation, the following rights must be granted:

- **CD_Users:**
  - Standard rights: View
- **CD_Designers:**
  - Standard rights: View
  - Advanced rights: Design Cube, Publish
- **CD_Admins:** Full control

#### Procedure

1. Log on to the Central Management Console and in the Manage section, click Applications.
2. Right-click the EPM Connection Manager application and select User Security.
3. Click Add Principals.
4. Select the "CD_Designers" group and add it to the right panel.
5. Click Add and Assign Security.
   The Assign Security window opens.
6. In the Access Levels tab, add the View right.
7. Click the Advanced tab.
8. Click the **Add/Remove Rights** link.

9. In the left pane, select the EPM Connection Manager application and in the right pane, select the **Design Cube** and **Publish** rights.

![Add/Remove Rights](image)

10. Click **Apply** and **OK**.

Back in the **Access Levels** tab, you can see the rights that have been assigned to the user.
11. Repeat the same steps for the “CD_ Viewers” but assign to the group the View right and then the Publish and Analyze advanced rights.

12. Repeat the same steps for the “CD_Admins” but assign to the group the Full Control right.

13. Click Close.

### 3.3.4 Configuring the EPM Connections

**Context**

By default, the CMC only displays objects to which you have access, so you do not see the EPM connections. This chapter explains how to define access rights to the folder containing connections. This enables you to define who will have rights to access or create connections to the BOE Cube Designer application.

A connection is a “correspondance” between an SSAS database or a Netweaver database, a Datapump URL to access this database, and a Financial Consolidation database identified through a web service.

For scenario 2 example provided in this documentation, the following rights must be granted:

- CD_ Viewers: View
- CD_Designers: Full Control
- CD_Admins: Full control
Procedure

1. Log on to the Central Management Console and in the Organize section, click EPM Connections.
2. Click Manage > Security > EPM Connection Folder Rights.
3. Click Add Principals.
4. Select the “CD_Designers” group and add it to the right panel.
6. In the Access Levels tab, add the Full control right.
7. Click Apply, then OK.
8. Repeat the same steps for the “CD_Admins”.
9. Repeat the same steps for the “CD_Viewers” group but assign this group the View right.

Results

You can then customize security for each single connection.

3.3.5 Configuring Web Intelligence Connections

Context

When installing the EPM Connection Manager with IPS (Information Platform Services), Web Intelligence and Universes are not available. The following chapter is intended only for a Cube Designer platform using the full BOE environment, and not for a platform using the IPS (Information Platform Services).
Procedure

1. Log on to the Central Management Console and in the Organize section, click Universes.
2. Select Manage > Top-Level Security and click All Universes.
   A warning message opens.
3. Click OK.
   The User Security: Universes window opens.
4. Click Add Principals.
5. Select the "CD_Viewers" group and add it to the right panel.
6. Click Add and Assign Security.
   The Assign Security window opens.
7. In the Access Levels tab, add the View right.

![Assign Security Window](image)

8. Click Apply, then OK.
9. Repeat the same steps for "CD_Designers" and "CD_Admins" but assign them the Full Control right.
10. Go back to the Home page and in the Organize section, click Connections.
11. Select Manage > Top-Level Security and click All Connections.
    A warning message opens.
12. Click OK.
    The User Security: Connections window opens.
13. Click Add Principals.
14. Select the "CD_Viewers" group and add it to the right panel.
15. Click Add and Assign Security.
    The Assign Security window opens.
16. In the Access Levels tab, add the View right.
17. Click Apply, then OK.
18. Repeat the same steps for "CD_Designers" and "CD_Admins" but assign them the Full Control right.
3.3.6 Configuring Access Rights on BI Launch Pad Folders

Context

If you want user groups to consult EPM Add-in workbooks via BI Launch Pad, you must configure access rights on the BI Launch Pad folders. By default, these folders cannot be accessed or seen.

You can grant the standard right "View" to all user groups, to enable users to connect to the web portal.

Using scenario 2, you create a sub-folder named Analytics, and grant those three user groups the "Full Control" right.

Procedure

1. Log on to the Central Management Console and in the Organize section, click Folders.
2. Select Manage > Top-Level Security and click All Folders.
   A warning message opens.
3. Click OK.
   The User Security: Root Folder window opens.
4. Click Add Principals.
5. Select the "CD_Viewers" group and add it to the right panel.
6. Click Add and Assign Security.
   The Assign Security window opens.
7. In the Access Levels tab, add the View right.
8. Click **Apply**, then **OK**.
9. Repeat the same steps for “CD_Designers” and “CD_Admins” groups.

### 3.3.7 User Rights Table

The following table summarizes the access rights that should be defined for each type of user group:

<table>
<thead>
<tr>
<th>Groups</th>
<th>Access in...</th>
<th>BI Launch Pad</th>
<th>Public folders</th>
<th>EPM connections</th>
<th>EPM Connection Manager application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>No access</td>
<td>Non applicable</td>
<td>Non applicable</td>
<td>Non applicable</td>
<td>Non applicable</td>
</tr>
</tbody>
</table>
3.4  Connecting to SSAS Cubes with Third Party Tools

You can connect to SSAS cubes that are deployed through Financial Consolidation with third party tools.

To do so, you must perform the following configuration:

- You must connect with users from a Windows Active Directory database
- The management of BOE users can only be Active Directory
- In the Financial Consolidation application, this user must be configured with the "use external authentication" option and the login must be set with the DOMAIN\USER syntax.

3.5  Connecting to Cube Designer using Single Sign On

To connect to Cube Designer using Single Sign On mode, the following is required:

1. Follow the steps provided in the Managing users using BusinessObjects Enterprise XI authentication [page 6] chapter of this guide:
   - In the Financial Consolidation Administration Console, configure the external authentication and select the Business Objects XI authentication.
   - In the Financial Consolidation application, create the users corresponding to the BusinessObjects Enterprise XI users in the Alias area, enter the exact same alias as the one provided in the properties of the BusinessObjects Enterprise XI user.

2. In the Cube Designer application, you must then set to TRUE the following key in the Cartesis.InformationDelivery.Workbench.exe.config file:

   ```xml
   <add key="IsSSOActivated" value="true" />
   ```

   **Note**

   Note that for now, all the accounts created in Financial Consolidation for SSO authentication needs, function only if the 'Use Windows Account' option is selected in the Financial Consolidation login screen. If the two steps above have been completed, when an end-user logs in to his computer, then launches Cube Designer, the logon dialog box still opens but the authentication information is already filled in. The user only needs to select the EPM Connection.
4 Configuring SAP Financial Consolidation Web with firewalls

SAP Financial Consolidation uses the following objects to communicate via the network using various protocols. Each of the executable processes requires at least one IP port.

SAP Financial Consolidation objects communicate using the following protocols:

Table 2:

<table>
<thead>
<tr>
<th>This component ...</th>
<th>Calls using...</th>
<th>Is called with...</th>
<th>... this component</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtBroker</td>
<td>DCOM</td>
<td></td>
<td>CtControler</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>CtServer</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td>DCOM</td>
<td>Financial Consolidation Web Administration Console</td>
</tr>
<tr>
<td>HTTP / HTTPS</td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Web Site</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Web Service</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Excel Link</td>
</tr>
<tr>
<td>CtServer</td>
<td>DCOM</td>
<td></td>
<td>CtBroker</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation</td>
</tr>
<tr>
<td>RDBM client</td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Database</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Web Site</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Financial Consolidation Web Service</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>Excel</td>
</tr>
<tr>
<td>CMS protocol</td>
<td>DCOM</td>
<td></td>
<td>BusinessObjects Enterprise</td>
</tr>
<tr>
<td>CtControler</td>
<td>DCOM</td>
<td></td>
<td>CtBroker</td>
</tr>
<tr>
<td>Finance</td>
<td>DCOM</td>
<td></td>
<td>CtBroker</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>CtServer</td>
</tr>
<tr>
<td>FC Web Site</td>
<td>DCOM</td>
<td></td>
<td>CtBroker</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>CtServer</td>
</tr>
<tr>
<td>FC Web Service</td>
<td>DCOM</td>
<td></td>
<td>CtBroker</td>
</tr>
<tr>
<td></td>
<td>DCOM</td>
<td></td>
<td>CtServer</td>
</tr>
</tbody>
</table>
The protocols described in the table above use the following ports:

- **HTTP / HTTPS protocol**: default port is 80, 443. It can use any other ports if you have modified the default settings.
- **RDBM client**: depends on your RDBM provider: for example: 1433 (for SQL), 1434 UDP (for SQL), 1521 (for Oracle). Refer to the RDBM documentation to find out more about the appropriate configuration for firewalls.
- **DCOM**: see the next chapter to find out more information about DCOM configuration with firewalls.
- **SSAS**: by default, port 2383. Refer to the SSAS documentation to find out more about the appropriate configuration for firewalls.
- **NW protocol**: by default, port 3300. Refer to the NetWeaver BW documentation to find out more about the appropriate configuration for firewalls.
- **CMS protocol**: it is based on CORBA, uses the 6400 port and dynamic ports. Refer to the BusinessObjects Enterprise documentation to find out more about the appropriate configuration for firewalls.

### 4.1 Configuring DCOM for firewalls

Because DCOM allocates IP ports dynamically by default to each executable process serving DCOM objects on a computer, it is “firewall-unfriendly”. If you want to use a firewall, you should configure the DCOM objects to use a
specific range of IP ports. You will then be able to identify which port will be called and configure the firewall accordingly.

Clients discover the port associated with a particular object by connecting to and using the services provided by DCOM’s Service Control Manager (SCM). The DCOM Service Control Manager always operates at a fixed network port on every computer, i.e. port 135.

Because DCOM uses dynamic IP ports, you must change the configuration of SAP Financial Consolidation objects so that they use a specific range of ports and SAP Financial Consolidation can pass the firewalls.

In the case of SAP Financial Consolidation, DCOM objects used may be configured to use specific IP ports. The only object that cannot be configured is the SAP Financial Consolidation Web connector, because this object is just a DCOM client, and not a DCOM server. It will therefore not be called up by an external program via DCOM.

You are not required to define a range of ports for Finance.exe and Excel because they are not DCOM servers and will not be called up by objects.

To use DCOM through firewalls, you must ensure that all of the computers can reach each other using DNS queries (with both IP addresses and Fully Qualified Domain Names recognized in both directions). For example, the Web server must be able to reach (ping) the application server by entering its full name e.g. fcserver.sap.com and vice versa.

To provide name resolution of network names to IP addresses, you may be required to modify the following files on each of the computers:

- LMHOSTS (Windows Name Resolution ou WINS).
- HOSTS file (DNS resolution FQDN)

You should open these files and add a row for each server you want to reach only if you encounter problems with the name resolution of the computers.

**Note**

All the port numbers indicated in this chapter are example, you can use any number from 1024 to 65535.

**Note**

The DCOM protocol does not work when address translation is used.

**Tip**

To find out more about using DCOM with firewalls, go to the following URL: http://www.microsoft.com/com/wpaper/dcomfw.asp.

### 4.1.1 Specifying the recommended configuration

**Context**

The simplest way of setting up a firewall with SAP Financial Consolidation is to specify the range of ports on the computers hosting the SAP Financial Consolidation servers. Contrary to previous versions of SAP Financial Consolidation, you no longer have to change the client computers’ DCOM configuration.
4.1.2 Specifying a range of ports in DCOM

Procedure

1. Run the dcomcnfg utility and select the Default Protocols tab.
   The following dialog box appears.

   ![Distributed COM Configuration Properties](image)
   
   **DCOM Protocols:**
   - Connection-oriented TCP/IP
   - Connection-oriented SPX
   - Connection-oriented NetBEUI
   - Connection-oriented Netbios over IPX

   ![Add port range](image)
   
   **Add port range**
   
   - **Port range:** 5000-5100

2. Select the TCP/IP protocol and click Properties.
3. The Properties for COM Internet Services dialog box appears.
4. Click on Add.
   The following dialog box appears.
5. Enter a range of ports between 1024 and 65535, then click OK.

Results

The range of ports will depend on the number of objects run on each computer.

Each DCOM object instance requires one port to run.

The CtBroker.exe and CtController.exe processes therefore use one port each. On the other hand, several CtServer.exe processes can run at the same time, either because an application is being recycled (one server is stopping and the other starting to replace the first one) or because several applications are hosted on the same server.

The following rule can be applied to determine the range of ports:

- CtBroker.exe: 1 port.
- CtController.exe: 1 port.
- CtServer.exe: 2 ports per application hosted on the server.

Example

A server acting as the data source manager and the application server hosting three SAP Financial Consolidation applications will use 8 ports:

- 1 for CtBroker.exe.
- 1 for CtController.exe.
- 2 x 3 = 6 for CtServer.exe.

Note

You can no longer configure SAP Financial Consolidation without a range of ports.
4.1.3 Diagram of the network traffic between the different components

4.1.4 Example of a firewall in use

In the example below, the HTTP server is installed on a DMZ (demilitarized zone) host.
The firewall connected to the HTTP server will accept inbound and outbound traffic through port 80 (HTTP).

The firewall located between the HTTP server and the other servers will accept:

- inbound and outbound traffic through port 135.
- traffic flowing towards the HTTP server through port 80.
- traffic flowing towards the data source manager through port 5000.
- traffic flowing towards the application servers through ports 5000-5100.

In the example above, there is no DNS server. The IP names and addresses of the different computers have therefore been added to the HOSTS files of the HTTP server, data source manager and application servers.
5 Restrictions on Uploading Attachments

To ensure security, you can specify whether end users are allowed to upload certain file types and if a virus scanning application (if installed) can perform a virus-scan on these file attachments.

In the Financial Consolidation installation folder, the AllowedExtension.txt file enables you to configure a blacklist or a whitelist and also contains the Virus scanning parameter.

```plaintext
# In this file, you can specify which file types can be uploaded to the server.
# You can choose between two authorization types:
# Blacklist - blocks all extensions defined in the following string.
# Whitelist - authorizes only the extensions defined in the following string.
#
WhiteList=.CSV;.DOC;.DOCX;.PDF;.RTF;.ODT;.TXT;.XLS;.XLSX;.XLSB;.ODS;.PPT;
PPTX;.PPS;.PPSX;.ODF;.JPG;.JPEG;.PNG;.BMP;.GIF;.TIFF;
#BlackList=.ade;.adp;.app;.asa;.ashx;.asmx;.asp;.bas;.bat;.cdx;.cer;.chm;.cmd;
.com;.config;.cpl;.crt;.css;.dll;.exe;.fxp;.hta;.htc;.htm;.ida;.idc;.idq;.ins;
.ips;.js;.jse;.ksh;.lnk;.mad;.maf;.mag;.mam;.mar;.mas;.mat;.mav;.mew;
.mdg;.mdf;.mde;.mdt;.mdw;.mdz;.mcx;.msh;.msh1;.msh2;.msh1xml;.msh2xml;.msi;
.map;.mat;.ops;.pcd;.pif;.pif;.prf;.pxg;.printer;.pat;.reg;.rem;.scf;.scr;.act;shb;shs;
.sht;.shtml;.soap;.stm;.url;.vbi;.vbe;.vbs;.ws;.wsc;.wsf;.wsh
#
# The Virus scanning parameter enables you to specify if all the attached files
# uploaded to the server
# must be scanned by the anti-virus installed on this server.
Virus scanning=true
```

You configure these two parameters as follows:

- **The whitelist parameter** is activated by default. The extension list is populated by default and can be modified.
  Each list can be activated by removing the # at the beginning of the line.

  - **Caution**
    Only one list can be activated.

  The restrictions apply to both the Windows and Web clients for attachments in packages, manual journal entries, consolidations and so on.

- **The Virus scanning parameter** is activated by default. If you want to deactivate the virus-scan on file attachments, you must set it to false or comment this parameter.

  - **Note**
    This parameter is only taken into account only if an antivirus application is installed. In that case, Financial Consolidation will automatically connect to it. If no antivirus is installed on the machine, the parameter will be ignored.
i Note

After modifying AllowedExtension.txt, you must restart the CtServer.
This chapter describes how you should configure the DCOM protocol in order to connect the client workstation to the application server. Configuring DCOM enables you to choose the mode of authentication between the workstations and the server. Otherwise it is not possible to establish communication between a workstation and the application server.

The DCOM protocol is based on Windows NetBIOS components. For DCOM to work, NetBIOS must therefore be able to run. The NetBIOS connection can be established between two computers only if the required access rights have been assigned. The connection must therefore be established with a Windows account that has certain rights. Both computers must recognize the logins used for the connection. If the computers are in the same domain and the account used to establish the connection is a domain account, the connection is authorized.

If the computers are not in the same domain or the account used to establish the connection is a local account on one of the computers, the same account (with the same login) must also exist locally on the other computer.

From Windows 2003 and Windows XP SP2, the concept of anonymous accounts was introduced. If an anonymous account is used and the DCOM objects are configured correctly, the two computers can communicate even though they are not in the same domain and do not have a common login.

Caution

If you use the anonymous settings for DCOM configuration, DCOM communications will no longer be encrypted.

Authorizing the “Everyone” group enables any account recognized by the computer to connect.

Tip

To test that this works, try to connect one server to the other via a shared folder. The connection opened will use the current Windows session and simply checks if a connection is possible.

You must therefore define the user accounts that will be used to configure the SAP Financial Consolidation objects’ DCOM properties and ensure that they can be used.

By default, the setup configures DCOM so that the application can function correctly when the Windows session is closed on the server. However, if you encounter problems, you may need to check that the DCOM settings are as indicated in the chapters below.

By default, the setup configures DCOM in encrypted communication mode. By default, communication will work only between servers that are part of the same domain forest.
6.1 Checking the default DCOM configuration defined by the SAP Financial Consolidation setup

Context

If you want to verify the DCOM configuration defined by the SAP Financial Consolidation setup, you should verify that your settings correspond to the table below.

1. Select Run in the Windows Start menu.
2. Enter dcomcnfg.exe and click on OK.
3. Select one of the applications belonging to SAP Financial Consolidation to verify their properties (CtBroker, CtServer, CtController or Financial Consolidation).

Table 3:

<table>
<thead>
<tr>
<th>Process</th>
<th>Tab</th>
<th>Options to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtServer</td>
<td>General</td>
<td><strong>Packet Privacy</strong></td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td><strong>Run application on this computer</strong> (if the option is not greyed out)</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>For the Launch and Activation Permissions and for the Access Permissions, select the Customize option and click Edit: allow all Permissions for the Everyone and the ANONYMOUS LOGON users.</td>
</tr>
<tr>
<td></td>
<td>Endpoints</td>
<td>Leave default settings</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
<td>This user: the DCOM account you indicated during the setup</td>
</tr>
<tr>
<td>CtController</td>
<td>General</td>
<td><strong>Packet Privacy</strong></td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td><strong>Run application on this computer</strong></td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>For the Launch and Activation Permissions and for the Access Permissions, select the Customize option and click Edit: allow all Permissions for the Everyone and the ANONYMOUS LOGON users.</td>
</tr>
<tr>
<td></td>
<td>Endpoints</td>
<td>Leave default settings</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
<td>The system account</td>
</tr>
<tr>
<td>CtBroker</td>
<td>General</td>
<td><strong>Packet Privacy</strong></td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td><strong>Run application on this computer</strong></td>
</tr>
<tr>
<td>Security</td>
<td>For the Launch and Activation Permissions and for the Access Permissions, select the Customize option and click Edit: allow all Permissions for the Everyone and the ANONYMOUS LOGON users.</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
|          | **Caution**  
|          | Do not modify the Configuration Permissions |
| Endpoints| Leave default settings |
| Identity | This user: the DCOM account you indicated during the setup |

<table>
<thead>
<tr>
<th>Financial Consolidation</th>
<th>General</th>
<th>Packet Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Run application on this computer</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>For the Launch and Activation Permissions and for the Access Permissions, select the Customize option and click Edit: allow all Permissions for the Everyone and the ANONYMOUS LOGON users.</td>
<td></td>
</tr>
</tbody>
</table>
|                         | **Caution**  
|                         | Do not modify the Configuration Permissions |
| Endpoints               | Leave default settings |
| Identity                | The interactive user |

<table>
<thead>
<tr>
<th>Import Export Users.exe</th>
<th>General</th>
<th>Packet Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Run application on this computer</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>For the Launch and Activation Permissions and for the Access Permissions, select the Customize option and click Edit: allow all Permissions for the Everyone and the ANONYMOUS LOGON users.</td>
<td></td>
</tr>
</tbody>
</table>
|                         | **Caution**  
|                         | Do not modify the Configuration Permissions |
| Endpoints               | Leave default settings |
| Identity                | The interactive user |
6.2 Specific DCOM configuration with different domains

Context

⚠️ Caution

This section explains you how to configure DCOM with different domains, but it will deactivate DCOM encryption. This configuration is not recommended.

The Windows default security settings prohibit remote non-authenticated DCOM access. As authentication between two computers which are not in the same domain is not possible, the launch permissions must be changed so that they include the ANONYMOUS login. There is no need, however, to change the computer access permissions as they include the login by default.

Procedure

1. Run the `secpol.msc` command.

The following window displays the local security settings.

3. Right-click on this line and click on Properties.
   The Launch Permission dialog box appears.
5. Click on Add.
   The following dialog box appears.

![Select Users, Computers, or Groups dialog box]

6. Enter ANONYMOUS LOGON in the text box and click on Check Names and then OK.
   The login has been added.
7. Check all the Allow options for this login and then click OK.

   **Note**
   You must then add the ANONYMOUS LOGON account to the CtServer and CtBroker processes.

8. Run the dcomcnfg.exe command.
   The Component Services window appears.
9. Select the CtBroker process and right-click on it to edit its properties.
10. In the CtBroker Properties dialog box, select the Security tab.
11. In the Launch and Activation Permissions groupbox, select the Customize option and click on the Edit button.
    The Launch Permission dialog box appears.
12. Click on Add.
    The following dialog box appears.
13. Enter ANONYMOUS LOGON in the text box and click on Check Names and then OK. The login has been added.

14. Check all the Allow options for this login and then click OK.

15. Also add the ANONYMOUS LOGON account in the Access Permissions groupbox.

**Note**

You must not change the Configuration Permissions groupbox options.

16. Repeat the same procedure for the CtServer process.

17. For all Financial Consolidation processes, you must then configure all objects as indicated in the Checking the default DCOM configuration defined by the SAP Financial Consolidation setup [page 41], but in the General tab, you must select None from the Authentication Level drop-down menu instead of Packet Privacy.

### 6.3 Configuring Internet Explorer

**Procedure**

1. Start Internet Explorer and select Tools > Internet Options.
2. Select the Advanced tab.
3. Under the Security heading, check the Allow active content to run in files on My Computer option.

**Note**

This configuration is necessary on the Businessobjects Finance server application and on the client with a Terminal Services configuration.
Note

This configuration is linked to the user’s Windows profile. If working with Terminal Services, it must be configured for each SAP Financial Consolidation user. For the server, the configuration should be performed on the profile corresponding to the account that runs the CtServer.exe process.
7 Encrypting the settings of the web.config file

Context

To enhance security, you can encrypt the login and password given in web.config files used in the different SAP Financial Consolidation applications. This is the method recommended by Microsoft for ASP.NET applications.

Procedure

1. Download the aspnet_setreg.exe file which is available at the following Microsoft address: http://download.microsoft.com/download/2/9/8/29829651-e0f0-412e-92d0-e79da46fd7a5/aspnet_setreg.exe

2. Run the following command:
   \aspnet_setreg.exe - k:SOFTWARE\Business Objects\MyWebService - u:"your_domain_name\your_user_name" -p:"your_password"

   i Note
   The registry key name given here can have a different value from Reporter, depending on the application you are deploying.

   This command will create 2 keys named username and password in the registry tree mentioned in the command line, and will store your login and password in encrypted form.

   i Note
   The aforementioned tree depends on your applications. If you want to encrypt several logins and passwords for several applications, you must create the appropriate registry keys.

3. Edit the web.config file and search for the following rows:

   <add key="DefaultLogin" value="your_domain_name\your_user_name" />
   <add key="DefaultPassword" value="your_password" />

4. Change these rows as shown below:

   <add key="DefaultLogin" value="Registry:HKLM\SOFTWARE\BusinessObjects\MyWebService \ASPNET_SETREG,username" />
   <add key="DefaultPassword" value="Registry:HKLM\SOFTWARE\BusinessObjects\MyWebService \ASPNET_SETREG,password" />

   Next, you must authorize the account that runs the .NET framework to access these new registry keys if your operating system is Windows Server 2003.
5. Open the Registry Editor.

6. Select the `HKEY_LOCAL_MACHINE\SOFTWARE\BusinessObjects\MyWebService\ ASPNET_SETREG` registry key and right-click `Permissions`.

7. Click `Add` and select the account that runs the ASP.NET framework and assign the `Read` permission to this account.

   ![Note]
   
   In Windows Server 2003, this account is called `Network service` by default.

8. Close the Registry Editor.

   ![Note]
   
   To find out more, please see the official Microsoft documentation at the following address: [http://support.microsoft.com/default.aspx?scid=kb;en-us;329290#5](http://support.microsoft.com/default.aspx?scid=kb;en-us;329290#5).
8 Installing X.509 certificates

Context

The SAP Financial Consolidation setup installs and uses two default X.509 certificates. With these default X.509 certificates, you can use the application in a test or a development configuration. If you are running SAP Financial Consolidation and SAP BusinessObjects Cube Designer in a production environment, it is recommended that you get a certificate from a commercial or free certification authority.

By default, these certificates are not activated. You must activate them in order to communicate with other products.

These two X.509 certificates are the following:

- The first one is used to sign communications between SAP Financial Consolidation and SAP BusinessObjects Cube Designer components.
- The second one is used to sign communications between application servers if you want to use the BFC Monitoring service, that enables you to open performance counters through the Windows Performance Monitor.

8.1 Installing the X.509 certificate for Cube Deployer

Context

SAP Financial Consolidation Cube Designer uses standard public key encryption to support authentication. This is a reliable way to establish a disconnected trust relationship between different modules in order to provide federated authentication.

In this respect, the Cube Deployer plays the role of a Security Token Server. Thus, the Cube Deployer component will generate and sign the security token. In order to do so, it uses the private key of an X.509 certificate installed on Cube Deployer. The corresponding certificate could be either a corporate certificate or a generated self-signed one.

To install X.509 certificate for the Cube Deployer component, the following steps are required:

Procedure

1. Install the public key of your certificate on the server hosting the CtBroker.
2. Install the private key of your certificate on the server hosting the Deployer component.
3. Assign the correct access rights on the certificate to the account that will run the CtBroker.
4. In the SAP Financial Consolidation installation folder, edit the CtBroker.config file.

5. Uncomment the parameter Certificate subjectName. If you want to use another certificate than the one installed by default, enter the parameters of your own certificate.

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://schemas.sap.com/2008/09/15/CtBroker/Configuration">
    <SharedTrustedCertificates>
        <!-- Uncomment next line to trust the default Extended Analytics X509 Certificate (intended for development or test platforms) -->
        <!-- <Certificate subjectName="CN=Extended Analytics Deployer, O=BOBJ, C=FR"/> -->
        <!-- Uncomment next line to trust the default BFC Monitoring Service (intended for development or test platforms) -->
        <!-- <Certificate subjectName="CN=BFC Monitoring Service, O=BOBJ, C=FR"/> -->
    </SharedTrustedCertificates>
    <DataSources>
    </DataSources>
</configuration>
```

6. Save and close the file.

7. Restart the CtBroker service.

8. On the Deployer server, open the web.config file and locate the following section:

```xml
<Certificate subjectName="CN=Extended Analytics Deployer, O=BOBJ, C=FR" store="My"/>
</SharedTrustedCertificates>
</configuration>
```

9. Enter the distinguish name of the certificate and save the file.

### 8.2 Installing the X.509 certificate for BFC Monitoring

#### Context

To install X.509 certificate for the BFC Monitoring component, the following steps are required:

#### Procedure

1. Install the public key on the server where the CtBroker component is installed.
2. Install the private key on the machine where the BFC Monitoring Service is installed.
3. Assign the correct access rights on the certificate to the account that will run the CtBroker.
4. In the SAP Financial Consolidation installation folder, edit the CtBroker.config file.
5. Uncomment the parameter `Certificate subjectName`. If you want to use another certificate than the one installed by default, enter the parameters of your own certificate.

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <SharedTrustedCertificates>
    <!-- Uncomment next line to trust the default Extended Analytics X509 Certificate (intended for development or test platforms) -->
    <!-- <Certificate subjectName="CN=Extended Analytics Deployer, O=BOBJ, C=FR"/> -->
    <!-- Uncomment next line to trust the default BFC Monitoring Service Certificate (intended for development or test platforms) -->
    <!-- <Certificate subjectName="CN=BFC Monitoring Service, O=BOBJ, C=FR"/> -->
  </SharedTrustedCertificates>
  </configuration>
```

6. Save and close the file.

7. Restart the CtBroker service.

8. On the machine where the BFC Monitoring Service is installed, open the `web.config` file and locate the following section:

```xml
<Certificate subjectName="CN=Extended Analytics Deployer, O=BOBJ, C=FR" store="My"/>
</SharedTrustedCertificates>
</configuration>
```

9. Enter the distinguish name of the certificate and save the file.
9 EPM Add-in for Microsoft Office Security Settings

9.1 User Rights

When the EPM add-in is executed from the BI Launch Pad, the user has the ability to publish Microsoft Office document on the BOE server. This action is available only if the user has a publication right. This right is defined on the BusinessObjects Enterprise server.

9.2 Connections

When connecting to a source defined on the BusinessObjects Enterprise server, the EPM Add-in for Microsoft Office client retrieves a security token from the BOE server that is transmitted to the data source provider as an additional parameter (custom data) in the connection string.

When connecting directly to the EPM Add-in for Microsoft Office client, the system first checks the credentials against the BOE server and if successful retrieves a security token that will be used as described above.

In both cases, the credentials are used to determine user rights concerning data and meta data. Only allowed meta data will be visible to the user, and only allowed data will be returned from queries.
Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).